

AMENDMENTS TO THE CLAIMS

1. (Original) A method comprising:
initializing a pseudo-random number generator (PRNG);
obtaining local seeding information from a host;
securely obtaining additional seeding information from one or more remote and
independent entropy servers; and
stirring the PRNG with the local seeding information and the additional seeding
information.
2. (Original) The method of claim 1, wherein the initializing a PRNG comprises
initializing the internal state of the PRNG with a random value.
3. (Original) The method of claim 2, wherein the random value is a seed.
4. (Original) The method of claim 1, wherein the securely obtaining seeding
information from the one or more remote and independent entropy servers is
repeated for redundant entropy servers.
5. (Original) The method of claim 1, wherein the one or more remote and
independent entropy servers maintain random state pool to supply the host with
the random value.
6. (Original) The method of claim 1, wherein the securely obtaining seeding
information from the one or more remote and independent entropy servers may
include using a privacy protocol.
7. (Original) The method of claim 6, wherein the privacy protocol comprises secure
sockets layer (SSL) protocol.



(Original) The method of claim 6, wherein the privacy protocol comprises transport layer security (TLS) protocol.

9. (Original) The method of claim 1, wherein the stirring the PRNG comprises producing a cryptographically random stream of bits.

Claims 10. -16. (Cancelled)

17. (Original) An entropy enhancing system comprising:
a local system comprising a pseudo-random number generator (PRNG); and
one or more remote independent systems comprising entropy servers.
18. (Original) The entropy enhancing system of claim 17, wherein the local system generates local seeding information.
19. (Original) The entropy enhancing system of claim 17, wherein the one or more remote independent systems generate remote seeding information.
20. (Original) The entropy enhancing system of claim 17, wherein the entropy servers are machines.
21. (Original) The entropy enhancing system of claim 17, wherein the entropy servers are software.
22. (Original) The entropy enhancing system of claim 17, wherein the local system gathers the local seeding information.
23. (Original) The entropy enhancing system of claim 17, wherein the local system securely gathers the remote seeding information.
24. (Original) The entropy enhancing system of claim 17, wherein the PRNG is stirred using the local seeding information and the remote seeding information.